AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A [[M]]method for monitoring [[the]] usage of a service by a communication device coupled to a smart card, said service being transmitted from a resource able to communicate with said communication device by way of a network, said service comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow ~~by a respective~~ using a first key, said first key being encrypted in the data flow and decrypted in the smart card by way of a second key stored in said smart card ~~or derived inside said smart card~~, the method comprising ~~characterized in that said method comprises the following steps~~:

[[a.]] [[A]] a counting step, in which a memory location stores a count of occurrences of decryption steps of said first key attached to the ~~a same~~ service,

wherein the counting step comprises:

receiving the first key encrypted by way of the second key;

determining whether the first key corresponds to a previously stored encrypted key;

when the first key corresponds to the previously stored encrypted key:

sending, to the communication device, a previously stored decrypted version of the previously stored encrypted key without performing the decryption of the received encrypted first key;

when the first key does not correspond to the previously stored key:

incrementing the counter;

decrypting the received encrypted first key to obtain a new decrypted first key to be used for decrypting data flow; and

storing the received encrypted first key and the new decrypted first key; and

[[b.]] [[A]] a using step, in which said counter is used to determine a service fee for use of said service.

2. (Previously Presented) Method according to claim 1, characterized in that the smart card stores a predetermined fixed number, and in that it comprises a comparison step in which the incrementing counter is compared to the predetermined fixed number for checking if the counter has reached or not the value of the fixed number; if yes, adequate action can be performed.

3. (Previously Presented) Method according to claim 1, characterized in that a command is sent to the smart card for renewing the second key.

4. (Previously Presented) Method according to claim 1, characterized in that a command is sent to the smart card for Resetting/Updating the counter.

5. (Previously Presented) Method according to claim 3, characterized in that said command is encrypted by a third key known by the smart card.

6. (Original) Method according to claim 2, characterized in that the action is the completion of decryption steps.

7. (Original) Method according to claim 1, characterized in that, each first key is sent periodically, and in that the amount of data is converted into time of use limiting the use of a service in time.

8. (Previously Presented) Method according to claim 4, characterized in that said commands are transmitted to the smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content.

9. (Currently Amended) A smartcard, able to receive services from a network, said services comprising a plurality of encrypted data flow, the use of said service comprising successive decryption steps of data flow by a respective first key, said first key being encrypted in the data flow and decrypted in said smart card by way of a second key stored in said smart card or derived inside said smart card, characterized in that smart card comprises a microcontroller able to perform the following steps:

[[a.]] [[A]] a counting step, in which a memory location stores a count of occurrences of decryption steps of said first key attached to the ~~a same~~ service,

wherein the counting step comprises:

receiving the first key encrypted by way of the second key;

determining whether the first key corresponds to a previously stored encrypted key;

when the first key corresponds to the previously stored encrypted key:

sending, to the communication device, a previously stored decrypted version of the previously stored encrypted key without performing the decryption of the received encrypted first key;

when the first key does not correspond to the previously stored key:

incrementing the counter;

decrypting the received encrypted first key to obtain a new decrypted first key to be used for decrypting data flow; and

storing the received encrypted first key and the new decrypted first key; and

[[b.]] [[A]] a using step, in which said counter is used to determine a service fee for use of said service.

10. (Cancelled)

11. (Previously Presented) Method according to claim 4, characterized in that said command is encrypted by a third key known by the smart card.

12. (Previously Presented) Method according to claim 5, characterized in that said commands are transmitted to the smart card by way of the communication device, said communication device including a program for authorizing the transmission of such commands without reading its content.

13. (Canceled)

14. (Previously Presented) Method according to claim 1, wherein the method further comprises upon reception of a management container:

performing a retrieval of the counter; and

sending management data to the resource through a protocol based in a point-to-point mechanism.

15. (Previously Presented) Method according to claim 1, wherein the method further comprises:

associating at least two counters to a particular service; and

resetting one of the at least two counters, wherein the other counter is not reset at the same time.

16. (Previously Presented) Method according to claim 1, wherein the resource communicates with said communication device over a network.

17. (Previously Presented) A method for monitoring use of a service by a communication device, comprising:

receiving, by a smart card coupled with the communication device, encrypted data flow as part of a service transmitted to the communication device by a resource over a network, and wherein the encrypted data flow comprises an encrypted first key and encrypted data;

determining whether the encrypted first key corresponds to a previously stored encrypted key;

when the encrypted first key corresponds to the previously stored encrypted key:

sending, to the communication device, a previously stored decrypted version of the previously stored encrypted first key without decrypting the received encrypted first key;

when the encrypted first key does not correspond to the previously stored encrypted key:

incrementing a counter, wherein the counter stores a count of occurrences of decryptions performed for encrypted keys associated with the service;

decrypting the encrypted first key using a second key stored on the smart card to obtain a decrypted first key to be used for decrypting the encrypted data; and

storing the encrypted first key and the decrypted first key,

wherein the counter is used to determine a service fee for use of the service.

18. (Currently Amended) The method according to claim 17, wherein the communication device [[will]] does not use the decrypted first key to decrypt the service received by the communication device when the counter exceeds a predetermined fixed number stored on the smart card.

19. (Previously Presented) The method according to claim 17, wherein a command is sent to the smart card for renewing the second key.

20. (Previously Presented) The method according to claim 17, wherein a command is sent to the smart card for updating the counter.

21. (Previously Presented) The method according to claim 20, wherein the command is transmitted to the smart card by way of the communication device and the communication device uses a program for authorizing the transmission of the command without reading its content.